<center>Claims</center>

What is claimed is:

1. A method for uniquely authenticating each replication of a plurality of soft-copy documents, said plurality of soft-copy

5 documents forming a group, comprising the steps of:;

   selecting one soft-copy document out of said group to become a carrier for an authentication code aimed at protecting said group;

   concatenating said plurality of soft-copy documents, said

10   concatenating including the step of using a canonical form of said selected soft-copy document;

   computing an authentication code from said concatenated plurality of soft-copy documents and a predetermined key;

   generating a random number; and

15   creating said carrier by combining said random number and said authentication code and marking said selected soft-copy document.

2. The method according to claim 1 wherein said step of concatenating uses all of said plurality of soft-copy documents

20 with the exception of said selected soft-copy document.

3. The method according to claim 1 wherein said step of concatenating is replaced by the step of picking up a single soft-copy document.

4. The method according to claim 1 wherein the creating said
5   carrier comprises the steps of:

splitting said selected soft-copy document into a first set of data and a second set of data on the basis of said authentication code;

utilizing said random number to mark said first set;

10   transforming said random number;

utilizing said transformed random number to mark said second set; and

reassembling said first set and said second set into said carrier.

15   **5.** The method according to claim 1 wherein said selected soft-copy document is a plain text document and said first set and said second set comprise sets of words from said plain text document.

6. The method according to claim 5 wherein said plain text
20   document is marked through the insertion of extra blanks.

7. The method according to claim 6 wherein the step of using said canonical form of said plain text document includes the step of:

    stripping all interword blank characters, in excess of one,

5   off said plain text document; thereby, obtaining said canonical form.

8. The method according to claim 4 wherein said selected soft-copy document is a plain text document and said first set and said second set comprise sets of words from said plain text

10 document.

9. The method according to claim 8 wherein said plain text document is marked through the insertion of extra blanks.

10. The method according to claim 9 wherein the step of using said canonical form of said plain text document includes the

15 step of:

    stripping all interword blank characters, in excess of one, off said plain text document; thereby, obtaining said canonical form.

11. The method according to claim 4 wherein said authentication code, said random number, said transformed random number are binary vectors fitting respectively in said selected soft-copy document, said first set and said second set.

5 **12.** The method according to claim 4 wherein said splitting step includes the steps of:

forming said first set with the words from said selected soft-copy document corresponding to the ones of said authentication code; and

10 forming said second set with the words from said selected soft-copy document corresponding to the zeros of said authentication code.

13. The method according to claim 1 wherein said computing step comprises the steps of:

computing said authentication code from said concatenated plurality of soft-copy documents, said key and a counter;

5   testing said authentication code for a prespecified range of zero values to one values;

if said code does not fall within said prespecified range:

incrementing said counter; and

resuming at computing step; and

10   if said code does fall within said prespecified range:

validating said authentication code; and

exiting said computing step.

14. The method according to claim 4 wherein said computing step comprises the steps of:

computing said authentication code from said concatenated plurality of soft-copy documents, said key and a counter;

testing said authentication code for a prespecified range of zero values to one values;

if said code does not fall within said prespecified range:

incrementing said counter; and

resuming at computing step; and

if said code does fall within said prespecified range:

validating said authentication code; and

exiting said computing step.

15. The method according to claim 4 wherein said transforming step includes:

hashing said random number;

reusing said random number; and

inverting said random number.

16. A method for checking said authentication code comprising the steps of:

obtaining an said authentication code;

splitting said carrier into a said first set and a said second set;

extracting a first pattern from said first set;

transforming said first pattern;

extracting a second pattern from said second set;

comparing said transformed first pattern and said second pattern; and

if matching:

  passing checking; and

if not matching:

  failing checking.

17. A system for uniquely authenticating each replication of a group of soft-copy documents, comprising:

a selection component for selecting one soft-copy document out of said group to become a carrier for an authentication code aimed at protecting said group;

a concatenation component for concatenating said plurality of soft-copy documents, said concatenating including the step of using a canonical form of said selected soft-copy document;

a processor for computing an authentication code from said concatenated plurality of soft-copy documents and a predetermined key;

a generating component for generating a random number; and

carrier marking means for creating said carrier by combining said random number and said authentication code and marking said selected soft-copy document.

18. The system of claim 17 wherein the carrier marking component comprises:

a splitter component for splitting said selected soft-copy document into a first set of data and a second set of data

5   on the basis of said authentication code;

a transformation component for transforming said random number;

a marking component for utilizing said random number to mark said first set and for utilizing said transformed random

10   number to mark said second set; and

an assembly component for reassembling said first set and said second set into said carrier.

19. A computer-like readable medium readable by machine tangibly embodying a program of instructions executable by the machine for uniquely authenticating each replication of a plurality of soft-copy documents, said plurality of soft-copy documents forming a group, said method comprising the steps of:

selecting one soft-copy document out of said group to become a carrier for an authentication code aimed at protecting said group;

concatenating said plurality of soft-copy documents, said concatenating including the step of using a canonical form of said selected soft-copy document;

computing an authentication code from said concatenated plurality of soft-copy documents and a predetermined key;

generating a random number; and

creating said carrier by combining said random number and said authentication code and marking said selected soft-copy document.